



plaintiff cannot prove any set of facts in support of its claims that entitles it to relief. *See Edwards v. City of Goldsboro*, 178 F.3d 231, 244 (4th Cir. 1999). Although the court must take the facts in the light most favorable to the plaintiff, it “need not accept the legal conclusions [the plaintiff would draw] from the facts.” *Giarratano v. Johnson*, 521 F.3d 298, 302 (4th Cir. 2008) (quoting *Eastern Shore Mkts., Inc. v. J.D. Assocs. Ltd. P’ship*, 213 F.3d 175, 180 (4th Cir. 2000)). The court may also disregard any “unwarranted inferences, unreasonable conclusions, or arguments.” *Id.*

The Rule 12(b)(6) standard has often been expressed as precluding dismissal unless it is certain that the plaintiff is not entitled to relief under any legal theory that plausibly could be suggested by the facts alleged. *See Mylan Labs., Inc. v. Markari*, 7 F.3d 1130, 1134 (4th Cir. 1993). Nonetheless, the plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007) (quoted in *Giarratano*, 521 F.3d at 302); *see also Wolman v. Tose*, 467 F.2d 29, 33 n.5 (4th Cir. 1972) (“Under the liberal rules of federal pleading, a complaint should survive a motion to dismiss if it sets out facts sufficient for the court to infer that all the required elements of the cause of action are present.”).

Thus, in applying Rule 12(b)(6), the court also applies the relevant pleading standard. Despite the liberal pleading standard of Rule 8, a plaintiff must include more than mere conclusory statements in support of its claims. *See Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009). The complaint must contain sufficient factual matter, accepted as true, to state a claim that is plausible on its face. *Iqbal*, 129 S. Ct. at 1949; *Twombly*, 550 U.S. at 570. The reviewing court need only accept as true the complaint’s *factual* allegations, not its legal conclusions. *Iqbal*, 129 S. Ct. at 1949; *Twombly*, 550 U.S. at 555.

Expounding on its decision in *Twombly*, the United States Supreme Court stated in *Iqbal*:

[T]he pleading standard Rule 8 announces does not require “detailed factual allegations,” but it demands more than an unadorned, the defendant-unlawfully-harmed-me accusation. A pleading that offers “labels and conclusions” or “a formulaic recitation of the elements of a cause of action will not do.” Nor does a complaint suffice if it tenders “naked assertion[s]” devoid of “further factual enhancement.”

To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to “state a claim to relief that is plausible on its face.” A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.

*Iqbal*, 129 S. Ct. at 1949 (quoting *Twombly*, 550 U.S. at 555, 556, 557, 570) (citations omitted); *see also Bass v. Dupont*, 324 F.3d 761, 765 (4th Cir. 2003) (holding that “[w]hile a plaintiff is not charged with pleading facts sufficient to prove her case, as an evidentiary matter, in her complaint, a plaintiff is required to allege facts that support a claim for relief.”).

### **BACKGROUND**

The complaint alleges that Miller and his assistant Kelley, while employed by WEC, were in contact with Arc Energy, a competitor of WEC. Dkt. 1 at ¶ 11. At Arc Energy’s direction, Miller and Kelley allegedly downloaded a substantial number of WEC’s confidential documents and emailed the documents to Miller’s personal email address. *Id.* at ¶¶ 12-14. After resigning from WEC, Miller used the confidential documents to benefit Arc Energy at the expense of WEC. *Id.* at ¶ 15.

Based on these allegations, the complaint asserts ten causes of action against Defendants including one based on federal law: a claim that Defendants violated the CFAA by obtaining confidential information from WEC without authorization or in excess of their authorization. *Id.* at ¶ 32. As to this claim, WEC alleges that although Miller and Kelley had permission to access the confidential documents (*Id.* at ¶ 8), WEC’s policies prohibit (1) downloading confidential and

proprietary information to a personal computer and (2) using any confidential information or trade secret unless authorized by WEC. *Id.* at ¶¶ 12 and 32. Further, WEC alleges that Miller and Kelley exceeded their authorized access by agreeing to share WEC’s confidential information with Arc Energy. *Id.* at ¶ 10.

## DISCUSSION

### I. CFAA CLAIM

The only federal claim in the complaint is founded on 18 U.S.C. § 1030 *et seq.*, the CFAA. Dkt. No. 1 ¶¶ 29-34. Although the CFAA is primarily a criminal statute generally intended to deter computer hackers, it permits private parties who suffer sufficient injuries as a result of a violation to bring a civil action. *A.V. ex rel Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009). Specifically, the statute provides that “[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action” when damages or losses meet or exceed \$5,000 in one year. § 1030(g).<sup>1</sup>

WEC asserts that Defendants violated sections 1030(a)(2)(C), (a)(4), (a)(5)(B), and (a)(5)(C) of the CFAA.<sup>2</sup> These sections provide a remedy against a party who:

- (2) intentionally accesses a computer without authorization or exceeds

---

<sup>1</sup> Section 1030(g) allows for a civil action upon a showing of one of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). WEC is relying on subclause (I) of subsection (c)(4)(A)(i) which requires a showing of “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” § 1030(c)(4)(A)(i)(I).

<sup>2</sup> WEC’s complaint quotes language from the CFAA and cites to “18 U.S.C. § 1030(3)(c), (a)(4) and (a)(5)(A)(ii) and (iii).” Dkt. No. 1 at ¶ 30. The quotations from the statute in the complaint do not match these citations, and, in fact, the citation to 1030(3)(c) does not correspond to any portion of the statute. The court, therefore, assumes that WEC’s citations were in error and considers the sections of the CFAA quoted by WEC in its complaint, sections 1030(a)(2)(C), (a)(4), (a)(5)(B), and (a)(5)(C).

authorized access, and thereby obtains

\*\*\*

(C) information from any protected computer;

\*\*\*

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ;

\*\*\*

(5) (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

Liability under the relevant sections requires, as a predicate, showing that an individual acted “without authorization” (all four sections) or “exceed[ed] authorized access” (two sections). WEC alleges that the CFAA was violated when, at the direction of Arc Energy, Miller and Kelley intentionally accessed WEC’s computer system to download confidential and proprietary information for the benefit of Arc Energy. Dkt. No. 1 ¶ 32. WEC alleges that “Miller and Kelly’s conduct constituted breaches of their fiduciary duties to WEC and therefore, they did not have authorization or exceeded their authorization.” *Id.*

For the reasons set forth below, the court concludes that WEC fails to state a claim for relief under the CFAA.<sup>3</sup> In order for WEC’s CFAA claim to succeed, the court would have to conclude that an employee acts “without authorization” or “exceeds authorized access” when he is “disloyal and acts in violation of [employer] policies prohibiting the *use* of confidential information for purposes other than the business of [the employer].” Dkt. No. 23 at 5 (emphasis added). As this

---

<sup>3</sup> WEC alternatively suggests that the court should hold the present motions in abeyance pending an opportunity for discovery. The court, however, has accepted all allegations in the complaint as true, and concludes that because WEC’s policies restrict use and not access, it cannot state a claim under the CFAA.

court has previously held, the plain meaning of the statute does not support such an interpretation.<sup>4</sup>

#### **A. Meaning of “Without Authorization”**

WEC alleges that, by downloading the confidential information and sending it to Miller’s personal email account, Miller and Kelley acted “without authorization” because they violated WEC’s policies prohibiting (1) downloading confidential and proprietary information to a personal computer or (2) using any confidential information or trade secrets unless authorized by WEC. Dkt. No. 1 at ¶¶ 32, 12.

The CFAA creates liability when an individual “accesses” a computer or a protected computer “without authorization.” The company policies at issue in this case do not restrict an employee’s ability to *access* data. Instead, they restrict how a WEC employee may *use* confidential information after accessing it. Because liability under the CFAA is based on access not use, Miller and Kelley’s intended use of WEC’s confidential information does not create liability under the CFAA. *See, e.g., LVRV Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009) (interpreting “without authorization” as being without permission or having permission rescinded, and concluding that an employee’s intended later use of information he has permission to access has no bearing on “authorization” to access it under the CFAA).<sup>5</sup>

---

<sup>4</sup> This case presents a set of issues very similar to those faced by this court in *Sloan Fin. Grp., LLC v. Coe*, No. 0:09-cv-02659-CMC, 2010 WL 4668341 (D.S.C. Nov. 18, 2010). In *Sloan*, the court held that because liability under the CFAA is based on access not use, an employee’s intended use of an employer’s proprietary data is not sufficient to create liability under the CFAA. *See infra* at pp. 8-9.

<sup>5</sup> As noted in *Sloan*, the court recognizes that there is a split of authority on this question. 2010 WL 4668341, at \*n.6. Under a line of cases referred to as the *Citrin* line, the determination of whether “authorization” exists turns on whether the person accessing the information breached a duty of loyalty. *See Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). The Seventh Circuit, in *Citrin*, held that an employee who violates the duty of loyalty by acting adversely

It is undisputed that Miller and Kelley were employed by WEC when they downloaded the confidential information. During that employment, Miller and Kelley were authorized to access WEC's computers and servers, which contained the confidential information at issue in this case.<sup>6</sup> The court assumes without deciding that Miller and Kelly violated company policies prohibiting employees from downloading and using confidential information without WEC's permission. This does not, however, change the result because the allegedly improper actions of downloading, emailing, and sharing information with a third party are distinct from the action of accessing the

---

to his employer's interests loses his authorization to access the employer's protected computer. *Id.* at 421. Three other federal circuits have held or noted that an employee acts "without authorization" or "exceeds authorized access" under the CFAA when he either acts disloyally to his employer or with interests adverse to his employer's. *See, e.g., United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) ("[A]n employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business"); *P.C. Yonkers Inc. v. Celebrations The Party and Seasonal Superstore LLC*, 428 F.3d 504, 510 (3d Cir. 2005) (recognizing that the CFAA's reach extends to actions against "former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001) (holding that employee exceeded authorized access by sharing confidential employer information with interests contrary to those of his employer).

While the Fourth Circuit has not ruled on the issue, recent district court opinions within the Fourth Circuit suggest "authorization" does not turn on an employee's intended use of information in a manner that is adverse to employer interests or policy. *See Océ North Amer., Inc. v. MCS Servs., Inc.*, No. WMN-10-CV-984, 2010 WL 3703277, at \*4 (D. Md. Sept. 16, 2010) (holding that while an employee remained employed by the company, he had authorization to use computers and computer software and that "copying software onto his own laptop may have been a violation of his employment agreement, but that does not constitute a violation of the CFAA"); *Cvent, Inc. v. Eventbrite, Inc.*, No. 1:10-cv-00481, 2010 WL 3732183, at \*4 (E.D. Va. Sept. 15, 2010) (noting that "a mere allegation that a defendant 'used the information [which it had been given lawful authority to access] in an inappropriate way' did not state a claim for relief [under the CFAA]") (quoting *State Analysis, Inc. v. Amer. Fin. Servs., Assoc.*, 621 F. Supp. 2d 309, 317 (E.D. Va. 2009)).

<sup>6</sup> There is nothing in WEC's complaint to indicate that Kelley was not provided the same access to WEC's confidential information as Miller. Neither is there any allegation that Miller and Kelley were prohibited from accessing any of the confidential information downloaded and later shared with Arc Energy.

information. At the point Miller and Kelley were allegedly accessing the confidential information, they were performing an action authorized by WEC. In short, accessing the confidential information did not involve accessing a computer “without authorization” under the CFAA. Therefore, Defendants were not acting “without authorization” when they accessed the confidential information.<sup>7</sup>

**B. Meaning of “Exceeds Authorized Access”**

In the alternative, WEC asserts that even if Miller and Kelley were authorized to access the confidential information, they exceeded that authorization by (1) accessing the confidential information on behalf of Arc Energy<sup>8</sup> and (2) violating company policy regarding confidential information.

WEC incorrectly argues that the CFAA does not define “exceeds authorized access” and crafts its own definition of the phrase. Using definitions from Dictionary.com, WEC argues that “exceeds authorized access” means “to go beyond the permission given by the party giving the access,” and, therefore, “using information obtained by access for a purpose to benefit a third party qualifies as going beyond the authorization.” *Id.* at 6-7. In fact, the CFAA defines “exceeds authorized access” as “to access a computer with authorization and to use such access to obtain or alter information on the computer that the accessor is not entitled so to obtain or alter.” 18 U.S.C.

---

<sup>7</sup> WEC’s CFAA claim against Arc Energy is dependent on its claim against Miller and Kelley who allegedly acted as Arc Energy’s agents in accessing WEC’s confidential information. There is no allegation that Arc Energy independently accessed WEC’s protected computers or confidential information.

<sup>8</sup> “WEC argues that “[b]y agreeing to work on behalf of a third party, Arc Energy, [Miller and Kelley] breached their duty of loyalty to WEC and forfeited their authorization to access information on WEC’s computers.” Dkt. No. 23 at 8.



§ 1030(e)(6). Thus, liability under the CFAA, based on an allegation that an employee exceeded authorized access, depends on whether the employee accessed information he was not entitled to access. WEC has not alleged that Miller or Kelley accessed information that they were not “entitled to access.” Therefore its allegation falls outside the scope of this portion of the CFAA.

**Access on Behalf of Third Party.** The argument that breaching fiduciary duties forfeits an employee’s authorization to access follows the *Citrin* analysis of the CFAA, which this court rejected in its order in *Sloan Fin. Grp, LLC v. Coe*, No. 0:09-cv-02659-CMC, 2010 WL 4668341 (D.S.C. Nov. 18, 2010). *See* n.4 *supra* (explanation of *Citrin* line of cases). There, this court joined the “critical mass” of cases holding that CFAA liability depends on actions taken by an employer in authorizing access to information rather than on an employee’s purpose or intended future use of that information that is adverse to the employer’s interests. *Sloan*, 2010 WL 4668341, at \*5; *see Lewis-Burke Assoc., LLC v. Widder*, No. 09-302, 2010 WL 2926161, at \*5 (D.D.C. July 28, 2010); *see, e.g., Cvent*, 2010 WL 3732183, at \*4; *Orbit One Com., Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); *Nat’l City Bank, N.A. v. Republic Mortg. Home Loans, LLC*, No. 09-CV-1550, 2010 WL 959925, at \*2 (W.D. Wash. Mar. 12, 2010); *Bell Aerospace Servs. Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010); *ReMedPar, Inc. v. AllParts Medical, LLC*, 683 F.Supp.2d 605, 611 (M.D. Tenn. 2010). Acting on behalf of a third party competitor is merely another form of acting with an intended future use that is adverse to the interests of one’s employer. WEC’s allegation that Miller and Kelley accessed the confidential information on behalf of Arc does not bring the actions of any of the Defendants under the scope of the CFAA. *See supra* n.6.

**Violating Company Policy.** For WEC to succeed on its claim that Defendants exceeded

authorized access by violating company policies, the court would have to adopt the Fifth Circuit's interpretation of "exceeds authorized access" as expressed in *United States v. John*, which suggests that, when an employee's purpose in accessing information is in violation of employer policies, he has exceeded authorized access. 597 F.3d at 273 (*supra* n.4). Even if the court adopted this interpretation, it would not fit the facts of this case. To the extent an employee's purpose is to violate an employer policy regulating *access* to information, the conclusion of the *John* court would be consistent with the language of the CFAA. For example, the Eleventh Circuit recently held that an employee of the Social Security Administration was liable under the CFAA for violating company policy "prohibit[ing] an employee from obtaining information from its databases without a business reason." *United States v. Rodriguez*, No. 09-15265, 2010 WL 5253231, at \*1 (11th Cir. Dec. 27, 2010). That policy controlled what information employees could access, and because defendant accessed Social Security information about individuals for a personal rather than business reason, the court held he had exceeded his authorized access. *Id.* at \*4.

However, in this case, WEC's company policies regulated *use* of information not access to that information. Thus, even if Miller and Kelley's purpose in accessing the information was contrary to company policies regulating use, it would not establish a violation of company policies relevant to access and, consequently, would not support liability under the CFAA.

A narrow reading of the statute is supported by the fact that the CFAA is primarily a criminal statute enacted by Congress to deter computer hackers and enhance the government's ability to prosecute computer crimes. *Vanderhye*, 562 F.3d at 645. Although there is a civil remedy available, there is no evidence that Congress intended the statute be used to help companies enforce their confidentiality or non-competition policies. *See Nat'l City Bank*, 2010 WL 959925, at \*4 ("There

is no reason to believe that Congress intended [the CFAA] to create a federal enforcement mechanism for corporate policies regarding document handling and retention.”). There are a variety of other legal remedies potentially available to an employer who finds that an employee has misused or misappropriated proprietary or confidential information.<sup>9</sup>

Additionally, where a statute has both criminal and noncriminal applications, courts should interpret the statute consistently. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). The Supreme Court cautions against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants. *See United States v. Bass*, 401 U.S. 336, 347-49 (1971). To interpret “authorization” or “exceeds authorized access” based on an employee’s purpose or based on whether the employee’s interests were adverse to the interests of his employer at the time of access would expand the reach of this statute well beyond its literal terms. This would be both confusing and antithetical to the rule of lenity which states, a court “will not interpret a federal criminal statute so as to increase the penalty that it places on an individual when such an interpretation can be based on no more than a guess as to what Congress intended.” *U.S. v. Seidman*, 156 F.3d 542, 559 (4th Cir. 1998).

### **C. Conclusion**

For the reasons set forth above, Defendants’ motions to dismiss the CFAA claim are granted.<sup>10</sup>

---

<sup>9</sup> *See, e.g.*, Dkt. No. 1 (asserting causes of action for breach of duty of loyalty, breach of implied duty of good faith and fair dealing, conversion, violation of South Carolina Unfair Trade Practices Act, tortious interference with actual and prospective contractual relations, civil conspiracy, constructive trust, and misappropriation of trade secrets).

<sup>10</sup> Because the court finds that WEC has failed to state a claim for relief under the authorization prong of the CFAA, the court need not reach the issues of whether WEC adequately

## II. SUPPLEMENTAL JURISDICTION

Assuming the CFAA claim is dismissed, Defendants ask the court to dismiss the remaining state law claims pursuant to the court's discretion under 28 U.S.C. § 1367. WEC has not filed any opposition to this aspect of Defendants' motions.

The court's jurisdiction over the state law claims is premised on supplemental jurisdiction. *See* 28 U.S.C. § 1367(a). The court may decline to exercise supplemental jurisdiction if it "has dismissed all claims over which it has original jurisdiction." 28 U.S.C. § 1367(c)(3); *see also Shanaghan v. Cahill*, 58 F.3d 106, 109 (4th Cir. 1995) ("The doctrine of supplemental jurisdiction indicates that federal courts generally have discretion to retain *or* dismiss state law claims when the federal basis for an action drops away.").

"[T]rial courts enjoy wide latitude in determining whether or not to retain jurisdiction over state claims when all federal claims have been extinguished." *Shanaghan*, 58 F.3d at 110. The Fourth Circuit has identified several factors for a court to consider when making this determination: (1) "convenience and fairness to the parties," (2) "the existence of any underlying issues of federal policy," (3) "comity," and (4) "considerations of judicial economy." *Id.* (citing *Carnegie-Mellon Univ. v. Cohill*, 484 U.S. 343, 350 n.7 (1988); *Growth Horizons, Inc. v. Delaware County*, 983 F.2d 1277, 1284 (3d Cir.1993)).

**Fairness.** A key fairness consideration is whether any applicable statute of limitations would prevent Plaintiff from refileing the dismissed state law claims in the appropriate state court. *See Ketema v. Midwest Stamping, Inc.*, 180 Fed. Appx. 427, 428 (4th Cir. 2006) ("[T]he dismissal may be an abuse of discretion where the state statute of limitations expired prior to dismissal of the

---

pled that it suffered damages or loss under the CFAA.

anchor federal claim.”). However, 28 U.S.C. § 1367(d) provides that “[t]he period of limitations for any [state law claim asserted under 1367(a)] . . . shall be tolled while the claim is pending [in federal court] and for a period of 30 days after it is dismissed unless State law provides for a longer tolling period.”<sup>11</sup> Therefore, the court’s dismissal of WEC Carolina’s state law claims will not result in WEC Carolina losing the opportunity to have its case considered on the merits.

**Other Factors.** The other factors, likewise, support dismissal. There are, for example, no federal policy or other federal issues remaining. Comity, therefore, favors dismissal because a state court is better suited to handle a matter involving only state law claims. The early stage at which the viability of the CFAA claim was raised and resolved also favors dismissal as any loss of judicial economy resulting from the dismissal will be minimal.

Accordingly, pursuant to 28 U.S.C. § 1367(c)(3), the court dismisses the remaining state law claims without prejudice.

---

<sup>11</sup> States are required to give effect to this federal tolling provision so long as the dismissed state law claims were properly asserted in federal court under 28 U.S.C. § 1367(a). *See Jinks v. Richland County*, 538 U.S. 456, 466 (2003) (holding that this section is constitutional even when it tolls the statute of limitations applicable to a cause of action brought against a State’s political subdivision and, therefore, implicates sovereign immunity).

**CONCLUSION**

For the reasons stated above, the court grants Defendants' motions to dismiss as to the CFAA claim. Under 28 U.S.C. § 1367(c)(3), the court dismisses the remaining state law claims without prejudice.

**IT IS SO ORDERED.**

s/ Cameron McGowan Currie  
CAMERON MCGOWAN CURRIE  
UNITED STATES DISTRICT JUDGE

Columbia, South Carolina  
February 3, 2011